International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Data Storage for Mobile Touch Pass and Bio-Touch Pass Pattern Character Drawing Using Fingertips

Jananee V[1], Golda Dilip[2]

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract:Authentication is essential when protecting financial transactions or maintaining authorized documents. Daily, passwords are still used for several purposes. However, they frequently lack appropriate security while acting alone. This initiative enhances password conditions by requiring users to sketch each character of the secret phrase rather than typing them as they usually would. Using biometric information as a second level of client verification advances the conventional confirmation methods reliant on Personal Identification Numbers (PINs) and One-Time Passwords (OTP). In our suggested approach, users draw the secret phrase's digits on the device's touch screen instead of entering them all. In our suggested biometric architecture, the discriminative power of each handwritten digit is thoroughly examined, along with the strength when lengthening the secret key and the number of enrollment tests. The new e-Bio Digit information base, which provides online transcribed digits from 0 to 9, was developed using a mobile phone and finger input. In our suggested method, clients draw the secret word's numbers on the device's touch screen instead of typing them in. In our suggested biometric architecture, the discriminative power of each transcribed digit is mostly thoroughly examined, as well as the robustness when lengthening the secret phrase and the number of enrollment tests. The new e-Bio Digit information base was created utilizing a mobile phone and finger input and comprises online handwritten digits from 0 to 9.

Keywords: Recurrent Neural Network, Dynamic Time Wrapping (DTW), Mobile Database, Bio Database.

1. Introduction

Techniques, Methodologies, Technology, and Policies work together to protect assets from attackers and maintain their secrets.The expansion of the internet has resulted in widespread consumer use. Users of smart devices regard them as a secure location for private information. A collection of tools that may be used to combat online threats is referred to as a "cyber defence system." There are several resources at your disposal. Cybersecurity threat detectors and blockers include Solar Winds Defence Event Manager, Intruder, Sparta Antivirus, LifeLock, Bit Defender Total Security, Malware bytes, and Mime Cast. They have a report outlining the attacks by the invaders. The number of dangers rises in direct proportion to Internet use. In addition to identifying and reducing present risks, the current policy also aims to stop the emergence of future ones. Network intrusion identification frameworks have evolved to track the sent and received packages in the organization. They range from signature-based frameworks that identify prominent attacks to irregularity-based frameworks that distinguish abnormalities from a standard conduct profile.

Penmanship-renowned structures can identify the capture from contact screens, computerized pens, scanners, photos, and paper archives. Statistical, structural, neural network and syntactic methods were employed online and offline. It is modified and generates the output as a virtual file, which is perfect for ensuring the correct entry and manipulation of the input. However, the main requirements of this tool are to classify the image of any handwritten text, which is likely to be in the shape of cursive, slanted, or block writing. Virtualizing our handwritten pattern helps us identify a block or cursive writing style. This is unusual because there is more interference between customers and the system. This paper's kind and popularity stand out as its most exciting and potent components. Characters using Feature Extraction will fit this comparison method. A series of layered realities that rely on raw truths to attainable realities make up this process. Applications that constantly need a penmanship prominence tool include document check and investigation, address understanding, managing postal bank tests, signature authentication, and security research. This outline looks into the many emerging techniques that promise a reduction in screening time while delivering more accurate distinguishing evidence.

2. HANDWRITTEN RECOGNITION APPROACHES

To ensure secure systems, a review will acquaint the principles of handwriting recognition techniques with various technologies and methods.

2.1 RECURRENT NEURAL NETWORKS TIME ALIGNED [2020]

Versatile Touch DB is a collection of 64K web-based user tests conducted over six security sessions by 217 clients using 94 different sophisticated mobile phone models. An extensive analysis of the suggested validation strategy considers both traditional and innovative validation approaches, such as Dynamic Time Warping (DTW) and Recurrent Neural Networks (RNNs).

[1]*Research Scholar, SRM Institute of Science and Technology (SRMIST), Vadapalani, Chennai, India. Email: jv9579@srmist.edu.in*
Orcid: https://orcid.org/0000-0002-3552-7406
[2]*Associate Professor, SRM Institute of Science and Technology (SRMIST), Vadapalani, Chennai, India. Email: goldadilip@gmail.com*
Orcid :https://orcid.org/0000-0001-5175-6957
** Corresponding Author Email: jv9579@srmist.edu.in*

A TA-RNN combines the DTW and RNN to create more robust, attack-resistant structures. The Mobile Touch DB and the e-Bio Digit DB data sets are used. Using a four-digit secret key and a single preparation exam for each participant.

We achieved a mistake rate of 2.38 per cent, outperforming traditional secret key-based systems. Two hundred seventeen clients with 94 different mobile phone models completed 64K web-based person tests. A console-based attack may advance 100%, and we would be unable to validate the client. The unassisted usage of cell phones is the focus of the Mobile Touch DB knowledge base. For each customer, we have six sessions from the scenario recorded. The Mobile Touch DB informational collection opens the door for a variety of applications: I) examine the discriminative power of novel human touch participation components, ii) advance standard mystery state affirmation structures by using touch biometric data as the second level of customer approval, and iii) distinguish how we collaborate with cells trustworthily to redesign consistent check systems. Three preliminary steps are taken into consideration: I) a character-by-character evaluation to assess each character's ability to discriminate, II) a character-by-character evaluation to assess the effectiveness of our suggested strategy as the length of the passwords increases from 1 to 9 characters, and III) a design update evaluation. The neuromotor cycles involved in developing touchscreens are distinctive elements that help get professional and accurate touch association signals. Touchscreen signals, the development of new techniques, people experiences, contact connection indications, and advancement of extra-produced correspondence processes are human-device association variables emphasized while supplying or observing special human social occasions. Our suggested touch screen personal expression may be based on Time Series, which is intended to be a Time Function. Two types of testing, Sen rolled and Stest signals connected to X and Y spatial bearings, are now employed to isolate a lot of 21-time restrictions. The entire time-limit strategy.

2.2 [2020] OPTICAL CHARACTER RECOGNITION

A significant amount of study has gone into creating an Android app for personal use that can interpret a text from photos. These days, it's common practice to save data from handwritten documents for later use. Taking a picture of the handwritten report and storing it in image format is a straightforward approach to protecting data. Optical character recognition is a technique for transforming handwritten documents into a digital layout. Pre-handling, division, work extraction, and post-handling are a few processes. Numerous studies have used OCR to identify people. This machine uses an Android phone to take a photo of the report, and OCR is used in similar ways to finish the process. It's essential to comprehend the characters used in different styles of handwriting. Consequently, a device has been developed to read handwritten documents and turn them into editable text. The records that must be written using the writer determine this machine's output. Our machine has a 90% accuracy rate regarding handwritten data, making it the finest tool for editing or sharing diagnosis documents. Sequential.

2.3 FLOATING FORWARD SEARCH (SFFS)

The two stages that make up the BioTouchPass biometric innovation are Feature Extraction, which employs temporal capabilities to separate elements, and BioTouchPass. An assortment of 21 transitory capabilities concerning kinematic, mathematical, and course data are divided for each digit using the signs captured by the digitizer (i.e., X and Y spatial directions). Sequential Forward Floating Search (SFFS) is utilized to identify the optimal subsets of time capabilities for each manually typed digit to increase framework execution up to EER. The following approach mainly uses a Siamese engineering and Bidirectional Long-Short Term Memory (BLSTM) to extract a uniqueness measure from data sets.

2.4.RECURRENT NEURAL NETWORKS AND DYNAMIC TIME WRAPPING:

We review and examine the benefits and drawbacks of the most recent research on contact biometrics for cell confirmation. The overwhelming commitments of this perception are related to our proposed engineering, the robust results obtained with appreciation to related examinations, and our trial discoveries. We include biometrics into cell validation that relies on secret phrase input. For the similitude calculation, two outstanding brand-new approaches are readied: I) Dynamic Time Warping (DTW), which is extensively used in many outstanding fields, such as penmanship and discourse; and ii) Recurrent Neural Networks (RNNs), which are specific profound learning-to-understand designs considered for displaying consecutive data with self-assured length. We evaluate the contact biometric device holistically by testing the discriminative power of each transcribed digit.

Along with establishing the length of the written by-hand secret key and the number of available enrollment tests based on the customer's indication, we also assess the robustness of our recommended method. We provide explicit information for the transmission of our suggested strategy on sophisticated PIN- and OTP-based validation frameworks, along with several techniques for secret phrase age. We get better outcomes than other check methods that use graphical passwords and handwritten signatures, as well as the most cutting-edge attacks on contact biometrics.

We introduce the original e-Bio Digit database, which requires online transcriptions of mathematical digits from 0 to 9 for 93 customers, captured on a mobile device via finger contacts. Uncommon classes of manually written numbers have been acquired, allowing you to capture intra-customer inconstancy. This database is accessible to everyone in the exams region. The remaining sections of the essay are organized as follows. Sec. The related efforts in contact biometrics for cell possibilities are summarised in II. Shows our suggested contact biometric device accordingly. The following procedure requires manually entered mathematical digits from zero to nine online. It is known as the spic and span e-Bio Digit information base. The trial procedure and the outcomes obtained using our suggested technique will be described individually. A modern PIN and OTP-based entire permission structure that includes hidden expression age processes are changing the information. After a few predetermination composition lines, the final determinations and variables are drawn in.Penmanship biometrics and Beyond Touch biometrics have developed into a wholly entertaining method of pressuring customers to use mobile devices [9], [18]& [20]. Table I lists the pertinent tactics used in this area. We include details on the confirmation method, highlights, classifiers, and datasets taken into consideration for each perception. Table I also consists of the overall results of the check for the two common types of fraud that are considered here: 1) impersonation assault, which occurs when the perpetrators know some information about the victim, and 2) irregular assault, which occurs when no information about the victim is known. Be aware that most computations and exploratory settings, such as the quantity and kind of training and data analysis, vary across the works presented. Table I should thus be decoded in remarkable expressions to look at fantastic possibilities of use that are primarily dependent on contact biometrics but, at this time, don't character computations.

2.5 SMARTPHONE TOUCH DATABASES [2019]

By asking users to draw each password number on the touch screen instead of entering them, the novel Mobile Touch DB database investigates the viability of incorporating contact biometrics into password authentication structures. One application that serves as the inspiration for our suggested method is the usage of net payments with credit cards. The bank often gives the individual a password (typically between 6 and 8 digits). The user must input this password to log in to the security platform.

Our recommended solution improves the current situation by introducing a second authentication component based on the person's biometric data when drawing the numbers. The main contributions of this inquiry may be summed up as follows: We show and describe how to obtain the new Mobile Touch DB database. With an average of 314 instances per user, the collection has about 64K online character samples created by 217 users utilizing 94 outstanding phone models. Customers had to draw all possible combinations of numbers (from 0 to 9), letters (54 total), uncommon symbols (8 total), and four-number passwords during each acquisition session (6). According to the purchase procedure, Mobile Touch DB allows for a maximum of six collected periods for each problem, with a minimum three-week delay between each period. This database looks at an unsupervised mobile setting with no limitations on posture, location, or technology. Users were free to download and use the purchasing app on their own devices.

By describing a benchmark analysis of biometric authentication at the new Mobile Touch DB database, we offer a simple technique to replicate. In two different trials, the discriminative capability of each character was assessed for each character. The robustness of our suggested strategy was evaluated for each character mixture as the password length increased from one to nine characters.

The Mobile Touch DB database opens the door to several novel applications, including analyzing the discriminative power of unknown human contact interplay dynamics, ii) enhancing conventional password authentication structures by including contact biometric data as the second level of person authentication, and iii) examining how we use mobile devices daily to improve usability. Mobile Touch DB can be used for research on touch screen biometric authentication as well as other topics, including user-structured effects and improvements in user-dependent handwriting recognition algorithms; ii) neuromotor approaches to writing on touch screens; iii) sensing factors in obtaining representative and clean contact interplay signals; iv) human device interplay factors regarding touchscreen signals and development of improved interaction techniques, and v) touch screen biometric authentication.

2.6 CNN [2019]

In GRCL, the word "intermittent" is used to imply profundity near recurrence. Repeating at a nearby time is the recurrence we wish to prevent. When a big responsive field uses GRCLs as an alternative to CNNs, insights concerning profundity may be generated close to time. The GRCLs generally follow the advice of using BLSTMs. The CNN layers are left alone, and we employ GRCLs as an opportunity for LSTMs. The adaptation only has feed-ahead connections as a result. We demonstrate that the combination produces basically precise LSTM-based systems2 B. Data Preparation For teaching, the adaption requests line photos (x) associated with their records (y). Physically commenting on manually written text-based content following images gathered from many sources is one technique to obtain such information. The cost of the most valuable data is controlled in this way. In any event, commenting is time-consuming and expensive. Additionally, it is not always possible to locate a sufficiently large number of images with hand-produced textual material. As a result, when it comes to directing many languages, the accessibility of physically organized material tends to be expressly limited. We explain how we used a sizable quantity of stroke data that had been gathered to create an online handwriting prevalence machine in the next section [10], [11]. This technique permits us to produce additional material at a substantially reduced cost. III. Information SYNTHESIS, RENDERING, AND DEGRADATION PIPELINE We use a variety of data sources to create the best affordable HTR machine. For example, we need access to a sizable amount of ink data for making an online handwriting prevalence machine [10], [11] in various languages. We are developing plans to extend our engine to numerous subjects and dialects. However, for the sake of this study, we are only looking at Latin material. We are also using a web penmanship union pipeline to work on this data with penmanship designs that aren't effectively addressed in the legitimate corpus. This data is provided in pictures using the delivery pipeline described below, tainted by using the same debasing channel we are using to demonstrate an OCR machine on fake typeset data. The coaching data also includes debased simulated typeset data to increase perceived precision on typeset printed material. Additionally, we include outdated image data from several open databases to improve the accuracy of renowned handwriting. Finally, we have a small amount of image data with recognizable street-level contemporary handwriting.

The 2019 release of CLDNN (CONVOLUTIONS, LSTMS, DEEP NEURAL NETWORK).The goal of manually produced literary substance line notoriety is to provide a progression of Unicode code components for the printed material transcribed into a married line image. If x is left alone, it will be a line image, and y will be a series of Unicode factors. We think the relationship between x and y is represented by the probabilistic version P(y|x). We extend the method described in [15] to variant P(y|x) by scaling the information photograph's peak to a decent length of forty pixels and destroying the sedation region down to brightness (dim scale). The handled picture is next processed thoroughly into a neural part to produce a 1-D collection of logits, each of which is compared to an individual or a spotless image. The population has a talent for using a CTC misfortune [2]. The form can handle photographs with varying widths (lengths).

The value of an individual-fundamentally based absolutely n-gram language form is combined with the logits value at derivation time in a log-direct manner. The bar looks for is used to observe the best standing result. We test with the following premier form designs: 1) LSTM-fundamentally based form: Current written by hand text-based substance line notoriety styles predominately use LSTMs and distinctive repeating neural organizations [3], [5]-[8], [16]-[18]. The CLDNN (Convolutions, LSTMs, Deep Neural Network) structure presented using the technique of approach for [19] revitalizes our interpretation. We use the beginning [20] style structure described in [15] for the convolutional layers. We employ between one and four stacked bidirectional LSTMs for the LSTM layers (BLSTMs). Because repeating designs are inherently sequential, they cannot fully utilize the parallelism provided by way of approach for gas pedals made up of GPUs and TPUs. As a result, local area models with the most convenient feed-ahead associations are preferred for a large-scale manufacturing device over those with intermittent connections. We take a cue from [21] and use 1-D gated repetitive convolutional layers (GRCLs)1 as feed-forward freedom to LSTMs to replicate the recurrency and gating component of LSTMs with a feed-forward structure (see Figure 1). For the time being, GRCL is a gating instrumented repeating convolutional network [22]. The recurrency is near to depth, and measurements generation is dealt with using the gating component, which is processed using a sigmoid actuation and sped up using the genuine RELU enactment.

2.7 SIGNDB DATABASE DEEP

The e-Bio Sign DS2 signature database is currently not being done. The design, acquisition devices, and writing tools are considered in the most popular database, Deep si. The Deep sign database whole consists of thousand five hundred and twenty-six (1526) users from all four different and most frequently used databases (i.e..MCYT, Bio secure ID, Bio secure DS2,e-Bio-sign DSI) [14]. A brief description of each database's features includes how input is drawn, how the session medium and time interval between them is managed, and how impostors and their types are introduced to the database structure. For more clarity, we look for specific references. As the MCYT DB has a total of twenty-five (25), an additional twenty-five (25) signatures and expert forgeries were given to each user in a block of five (5) signatures throughout the course of one session. As users arrived, they were asked to have an ink pen and write their signature down on the paper as valid in the signing space. The signed document was then placed on the Wacom Intuits A6 USB pen tablet that records the two variety of signals, i.e. X and Y spatial co-ordinal points with a resolution of 0.25mm, and pressure of 1024. There are currently 330 users whose signatures were collected, considering over a controlled and supervised head person. Therefore, it should be assumed that all of these fake static signatures only provide forgers access to the signature area of the target picture. Sixteen (16) authentic signatures and twelve (12) professional signatures for each user were collected for the Bio Secure ID DB in four distinct levels of sessions, with a two-month gap between each user. Together, there are 400 users. In an office-like setting, pen-down signatures were collected, regulated, and moved on with the supervisor.

The Wacom Intuos 3 pen tablet records two types of signals, i.e., X and Y spatial co-ordinal points with a resolution of 0.25mm, the pressure of 1024 levels, orientations of the pen angular with azimuth and altitude angles, with a timestamp of 100Hz were adding to the pen-up trajectories are available. As users enter, they are asked to have an ink pen and write down their signature on the paper as valid in the signing space. According to these forgers, the static and dynamic signatures will be included in the first two partitions. The final portion of sessions for the signatures is regarded as part. Forgers only have the authorization to access the dynamics of the picturized partition. The BioSecure DS2 DB contained 650 users, with 30 genuine and 20 fake signatures for each head of the user. The signatures were collected in an office setting under the supervision of each leader in two separate sessions, with the third period between sessions. Users were instructed to sign documents while seated on a sheet propped up on the Wacom. The imposters, which are only used for dynamic forgeries by the e-Bio Sign DS1 database[2], come in five different device types, with three specifically designed for recording handwritten data (Wacom STU-500, STU-530, and DTU-1031). In contrast, the other two are used as general-purpose tablets.

Additionally, all five of these devices are pen-stylus-equipped. Additional software for the two Samsung devices reads input with a finger and analyses how writing input affects system performance. All five devices used the same recording protocol, were placed on the desktop, and could be oriented in whichever was most comfortable for the posture.

The software for capturing handwriting and signatures was created for all devices in the same manner to follow the current trend.

In the virtualization acquisition procedure, signatures were collected over two sessions, with a minimum of three weeks between sessions for each of the 65 subjects. There are eight genuine signatures for each user and reader and six skilled forgeries. When using a stylus to read input, timestamps, pressure, and coordinates are recorded for the corresponding devices; however, added Pen-Up trajectories are only recorded as input in the connected devices when the finger has been the input. Both dynamic and static forgeries have been detected. The first of the three is a Wacom Stu-530 built primarily for capturing data written by hand. The second is a Samsung Galaxy Note 10 tablet, a typical all-purpose tablet, and the third is a Samsung Galaxy S3 smartphone. All three devices were tracked over three weeks by being kept on a table, recorded with a stylus, and accurately noted the time between each device. The Samsung Galaxy S3 phone's signature was also strategically recorded using a pen. The user can create a virtualize for the dynamic realization for the recorded signature to repeat it whenever they need to perform the highest quality of forgeries. Recorded signatures were deposited into two sessions for every 81 users with a minimum time interval of three weeks.

2.8.Profound analysis and multi-feature extraction from 2015

In computer vision and pattern recognition, handwritten digit popularity is an important research topic. In this research, a powerful handwritten digit popularity method is proposed, which is based entirely on specific multi-characteristic extraction and in-depth analysis. We first pre-process images of various sizes and stroke thicknesses to avoid alarming statistics and maintain valuable capabilities. Second, given that the popularity of handwritten digit photographs is unique to traditional image semantics, we provide particular characteristic definitions, such as form, distribution, and projection capabilities. Additionally, we include a few skills into deep neural networks for semantics popularity. The results of our experiments on the benchmark database of MNIST handwritten digit images demonstrate our set of rules' excellent overall performance and its superiority to several existing techniques.

2.92011 SVM/ANN

After segmenting each letter into its parts, a heuristic approach is used by processing neural networks, testing the Multilayer Perceptron (MLP), Radial Basis Function (RBF), and Support Vector Machine (SVM), and selecting the most correct one. The deconstruction technique enables us to partition handwritten text by combining two methodologies that use heuristics and artificial intelligence. Black-and-white picture to 0s and 1s transformation. The second procedure continues by carrying out tilt detection in the manner described in [9] and tilt correction. The image rotates using this way from -45 to 45 degrees. The Wigner-Ville distribution is computed at each rotation through a horizontal projection. The angle that indicates the highest intensity following the application of WVD is chosen as the predicted tilt angle. WVD functions as Time Frequency Coupling and its projection of data. Heuristic methods are employed to find suggested segmentation sites in handwritten texts during the training and testing stages. Try to identify the characteristics in each word that correspond to the segmentation points. A. Heuristic segmentation An easy heuristic segmentation technique is practised, scanning handwritten texts to find good segmentation sites between letters. The basis for segmentation is figuring out the minimal distance between letters or the location of an arc. Italics written by hand often look like this. A histogram of the vertical pixel density is looked at for this purpose. It can show where potential segmentation spots inside a word could be. But other characters, like "a" and "o," might indicate the wrong segmentation points. As a result, it features a "hole search" feature that crosses over the segmentation points that go through the "hole". When the distance between the previous segmentation point and the checked location is higher than or equal to the average character width, the algorithm concludes that the two segmentation points are not excessively near. Makes a check. In contrast, a new segmentation point will be added in the contour area with few segmentation points. Marking Segmentation Points Manually We have built a neural network segmentation training database. 26 English words, including capital and lowercase letters, were chosen. Ten examples of each term from various writers were then compiled on paper. I pre-processed the image after scanning it to get a list of 260 words. Heuristic function detectors segregate all terms once the working ANN is processed. The "right" segmentation point classes and "incorrect" segmentation point classes may be distinguished in the segmentation point output from 115 using the heuristic feature detector. To assess the density of black and white pixels, the feature extractor first extracts a matrix of pixels that represents the segmentation region. It next divides this matrix into tiny windows, each measuring 5x5 pixels in size. Each 5x5 window's black pixel density value is recorded in the training file as the window's value. The intended output is also included in the training file along with each matrix (0.1 for incorrect segmentation points, 0.9 for correct issues). Using a multilayer forward neural network (MFNN) trained with a backpropagation method, artificial neural network (ANN) training aids with step-by-step navigation. An ANN is given the training file created in the previous stage. Heuristic algorithms are employed to segment the words in the test, like how ANNs are trained and tested. Automatic segmentation points extraction and transmission to the trained ANN. After then, ANN determines if each segmentation point is true or false. After ANN validation, assessment requires successful segmentation of data points.

2.10 APPROACHES FOR NEURAL NETWORKS [2011]

The study defines an offline handwritten alphabetical character recognition system using multilayer feed-forward neural networks. A novel technique known as diagonal-based function extraction is presented for extracting the handwritten alphabets' functions. The neural community is educated using 50 data sets containing 26 alphabets written by various people and tested using 570 unique handwritten alphabetical letters. Compared to systems employing the conventional horizontal and vertical techniques of function extraction, the suggested reputation device functions pretty correctly and produces superior stages of reputation accuracy. This gadget could help convert handwritten papers into structural text content forms and identify handwritten names. It defines the suggested reputation device. Pre-processing, segmentation, function extraction, class and reputation, and post-processing steps are part of a standard handwritten reputation device.

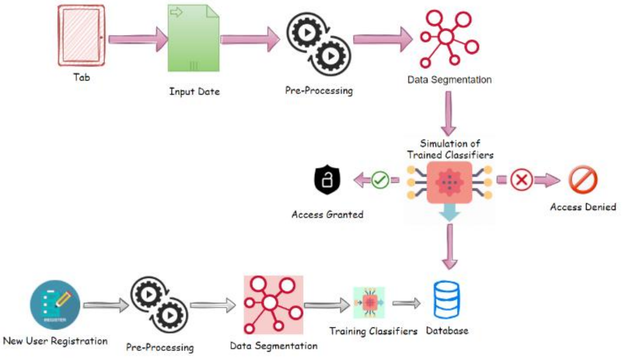
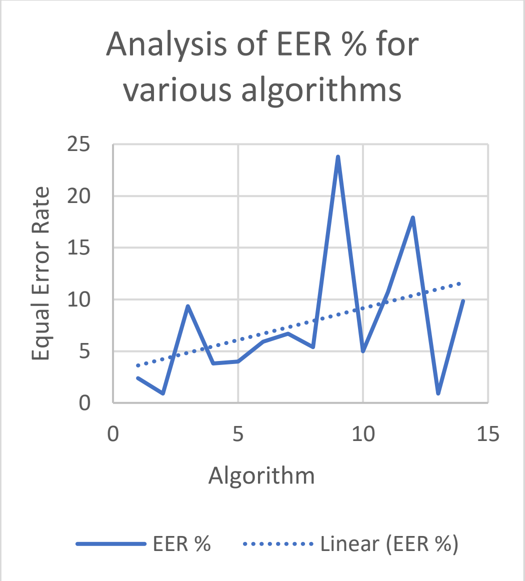


Fig 1. Data Flow Through Handwritten Methods

3 GRAPHICAL REPRESENTATION OF ANALYTICS



4. CONCLUSION

The many strategies for offering a safe password-based authentication system are discussed in this book. With an equivalent mistake rate of 2.38 per cent, the time-aligned recurrent neural network technique is effective for handwritten digit-based passwords. The other approaches are based on neural networks, which have accuracy rates between 97.8 and 98.5 per cent for various characteristics. The databases used by the models mentioned in this article range from 93 to 60000 datasets and users. The databases MobileTouchDb and DeepSignDbare have datasets of handwritten text that were gathered from 217 and 1526 individuals, respectively. The models may be trained and tested using these databases. DeepSignDb has a false rejection rate of 0.5

percent, a false acceptance rate of 20 percent for the finger, and a false error rate of 4 percent for the pen. MobileTouchDb gives an equivalent mistake rate of 5.9 ppercent The study analyses the outcomes, benefits, and drawbacks of numerous strategies and algorithms used to improve conventional password-based systems.

Table 1:ANALYTICAL REPORT BASED ON THE SURVEY

Classifier	Results	Password Pattern	Training Samples	Participant count
Time Aligned Recurrent Neural Networks [2020]	2.38% error rate	Handwritten digits	MobileTouchDb, e-BioDigitDb	217 users
Optical Character Recognition [2020]	90% accuracy	Pictures of handwritten records that is converted into editable text.	pictures of handwritten text	-
DeepWriteSYN: On-Line Handwriting Synthesis via Deep Short-Term Representations	9.36%	Handwritten digits	DeepWriteSyn Database	-
Forward Floating Search (SFFS) [2019]	3.8% Equal Error Rates	Picture of handwritten digits	e-bioDigitDb	93 users
DYNAMIC TIME WRAPPING AND RECURRENT NEURAL NETWORKS [2019]	4.0% Equal Error Rates (EERs)	Handwritten digits	e-bioDigitDb	93 users
MOBILE TOUCH DATABASES [2019]	5.9% Equal Error Rates (EERs)	Handwritten digits	MobileTouchDb, e-BioDigitDb	217 users
CNN [2019]	6.69% EER	Handwritten Document Character Recognition	CEDAR	500 Users
CLDNN (Convolutions, LSTMs, Deep Neural Network) [2019]	False Rejection 5.4% to 4.0 %	Handwritten Word Recognition	IAM Online Handwritten Database	508 images with 4868 lines
DEEPSIGNDB DATABASE [2019]	False rejection rate is 0.5% False acceptance rate is 20% for finger and 4% for pen	Handwritten digital signature	Data of 1084 users in DeepSignDb is used for training and 442 users for testing	1526 users
Handwritten One-time Password Authentication System Based On Deep Learning [2019]	98.58% accuracy in the handwriting recognition task and about 93% accuracy in the writer verification task based on four handwritten digits	Handwritten digits	NIST Handprinted Forms and Characters Database	3500 users
Touch gesture-based active user authentication using dictionaries	EER ranging from 0.4% to 23.8%	Touch based input	face-based mobile active authentication data sets	Public dataset
Incorporating Touch Biometrics to Mobile One-Time Passwords: Exploration of Digits [2018]	EERs ca. 5.0% when using skilled forgeries	Handwritten digits	e-bioDigitDb	93 users
Exploring RNN for On-Line Handwritten Signature Biometrics [2018]	5.0% Equal Error Rate (EER) for skilled impostors.	Handwritten signature	BiosecurID database	400 users
Benchmarking Touchscreen Biometrics for Mobile Authentication	EER = 10.7%	Touchscreen gestures	Serwadda Database Frank Database	190
Benchmarking desktop and mobile handwriting across COTS devices: The e-BioSign biometric database	EER = 17.9%	Handwritten text input	E-biosign database	75
Graphical Password-Based User Authentication With Free-Form Doodles [2016]	Equal error rates between 3% and 8% are obtained against random forgeries and between 21% and 22% against skilled forgeries	Handwritten Doodle based input	DooDB database	100 users
Active User Authentication for Smartphones: A Challenge Data Set and Benchmark Results [2015]	EER ranging from 22% to 38%.	Handwritten text	Active Authentication Dataset	-
Multi-feature Extraction and Deep Analysis [2015]	-	MNIST handwritten digit pictures	MNIST Dataset	60000 samples
SVM/ANN [2011]	0.1 for an incorrect segmentation point and 0.9 for a correct point	Handwritten words	Database containing 26 alphabets and 260 words	260 words
Neural Networks Approaches [2011]	recognition accuracy of 97.8 % for 54 features and 98.5% for 69 features	Handwritten alphabets	570 different handwritten alphabets and 50 sets of 26 alphabets each	50 information sets

REFERENCES

[1]. "BioTouchPass2: Touchscreen Password Biometrics Using Time Aligned Recurrent Neural Networks IEEE," by Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia, appeared in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 15, 2020.

[2]. Nouby M. Ghazaly, M. M. A. . (2022). A Review on Engine Fault Diagnosis through Vibration Analysis . International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 01–06. https://doi.org/10.17762/ijrmee.v9i2.364

[3]. International Journal of Computer Science and Information Technology (IJCSIT), Volume 3, Number 1, February 2011, DOI: 10.5121/ijcsit.2011.3103

[4]. J. Pradeep, E. Additionally, S. In the 12th International Conference on Fuzzy Systems and Knowledge (2015), Himavathi published "DIAGONAL BASED FEATURE EXTRACTION FOR HANDWRITTEN ALPHABETS RECOGNITION SYSTEM USING NEURAL NETWORK."

[5]. Hong Zhang Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System Wuhan, China Caiyun Ma College of Computer Science and Technology Wuhan University of Science and Technology Wuhan, China "Discovery (FSKD) Effective Handwritten Digit Recognition Based on Multi-feature Extraction and Deep Analysis" in Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020) IEEE X.

[6]. Prof. Vaibhav. Handwritten Character Recognition to Obtain Editable Text" in the 2020 International Conference on Electronics and Sustainable Communication Systems by V. Mainkar, Mr Ajinkya B. Upade, Ms Jyoti A. Katkar, and Ms Poonam R. (ICESC).

[7]. Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[8]. "Offline Handwritten Character Recognition Using Neural Network2011" by Anshul Gupta, Manisha Srivastava, and Chitralekha Mahanta was published in the International Conference on Computer Applications and Industrial Electronics (ICCAIE 2011)2019 International Conference on Document Analysis and Recognition (ICDAR)

[9]. R. A Scalable Handwritten Text Recognition System, Reeve Ingle, Yasuhisa Fujii, Thomas Deselaers, Jonathan Baccash, and Ashok C. Popat Google Research Mountain View, CA 94043

[10]. M. In the 2019 IEEE, Rajalakshmi, P. Saranya, and P. Shanmugavadivu published "Pattern Recognition - Recognition of Handwritten Document Using Convolutional Neural Networks."

[11]. S. Jenefa Jemima, "Secured Data Retrieval In Disruption Tolerant Military Networks Using Cp-Abe," International Journal of Engineering and Management Research, Volume 5, Issue 2, pp. 704–711, 2015.R. Tolosana and R. J. and Vera-Rodriguez Handwritten passwords for touchscreen biometrics: Fierrez, IEEE Trans. 10.1109/TMC.2019.2911506, Mobile Computing PP(99)

[12]. Javier Ortega-Garcia, Aythami Morales, Julian Fierrez, Ruben Tolosana, "Do You Need More Data? The IEEE Sept 2019 International Conference on Document Analysis and Recognition, "The DeepSignDB On-Line Handwritten Signature Biometric Database" (ICDAR)

[13]. R. A Scalable Handwritten Text Recognition System by Reeve Ingle, Yasuhisa Fujii, Thomas Deselaers, Jonathan Baccash, and Ashok C. Popat was presented at the 2019 International Conference on Document Analysis and Recognition (ICDAR) in Mountain View, California.

[14]. Hermina, J. ., Karpagam, N. S. ., Deepika, P. ., Jeslet, D. S. ., & Komarasamy, D. (2022). A Novel Approach to Detect Social Distancing Among People in College Campus. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 153–158. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/1823

[15]. Yang, J.-P. . "A Novel Storage Virtualization Scheme for Network Storage Systems". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 1, Jan. 2022, pp. 08-13, doi:10.17762/ijritcc.v10i1.5514.

[16]. "Pattern Recognition of Handwritten Document Using Convolutional Neural Networks" IEEE 2019 International Conference by M. Rajalakshmi, P. Saranya, and P. Shanmugavadivu, Professor Scholar Dept. of Computer Science and Applications Gandhigram Rural Institute

[17]. Rathidevi, "Secure multi-owner data sharing for dynamic groups in the cloud," International Journal of Innovations in Engineering Research and Technology, vol. 2, no. 5, 2015, pp. 2394–3696.

[18]. Exploring Recurrent Neural Networks for Online Handwritten Signature Biometrics, Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia, Biometrics and Data Pattern Analytics (BiDA) Lab-ATVS, Universidad Autonoma de Madrid, 28049 Madrid, Spain, 2018.

[19]. Chaudhary, S. . (2022). On the Minimality of Leibniz Isomorphisms. International Journal on Recent Trends in Life Science and Mathematics, 9(1), 11–18. https://doi.org/10.17762/ijlsm.v9i1.137

[20]. Javier Galbally, Julian Fierrez, and Marcos Martinez-Diaz, "Graphical Password-Based User Authentication With Free-Form Doodles," IEEE Transactions on Human-Machine Systems, Vol. No. 46, August 2016, page 4

[21]. "Investigation on Touch Biometrics: Behavioural Factors on Screen Size, Physical Context, and Application Context" in 978-1-4799-1737-2/15/$31.00 2015 IEEE 2015 by Tao Feng, Xi Zhao, Nick DeSalvo, Tzu-Hua Liu, Zhimin Gao, and Weidong Shi

[22]. U. Mahbub, V. M. Patel, S. Sarkar, and R. "Active user authentication for smartphones: A challenge data set and benchmark results," by Chellappa, Proc. IEEE BTAS, pp. 1–2, 2016.

[23]. J. M. Martinez-Diaz, J. Galbally, A. Pozo, Fierrez, and A. Benchmarking Touchscreen Biometrics for Mobile Authentication, IEEE Transactions on, Morales on Information Security and Forensics, vol. 13, 2018

[24]. "DeepWriteSYN: Online Handwriting Synthesisvia Deep Short-Term Representations," Ruben Tolosana, Paula Delgado-Santos, Andres Perez-Uribe, Ruben Vera Rodriguez, Julian Fierrez, and Aythami Morales

[25]. N. A. Libre. (2021). A Discussion Platform for Enhancing Students Interaction in the Online Education. Journal of Online Engineering Education, 12(2), 07–12. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/49